



Hybrid, Multi-cloud Management Maturity

How Leaders Tame Complexity, Increase
Efficiency, and Innovate at the Speed of Business

Adam DeMattia | Senior Director, Research

John Grady | Principal Analyst, Network Security

ENTERPRISE STRATEGY GROUP

APRIL 2024

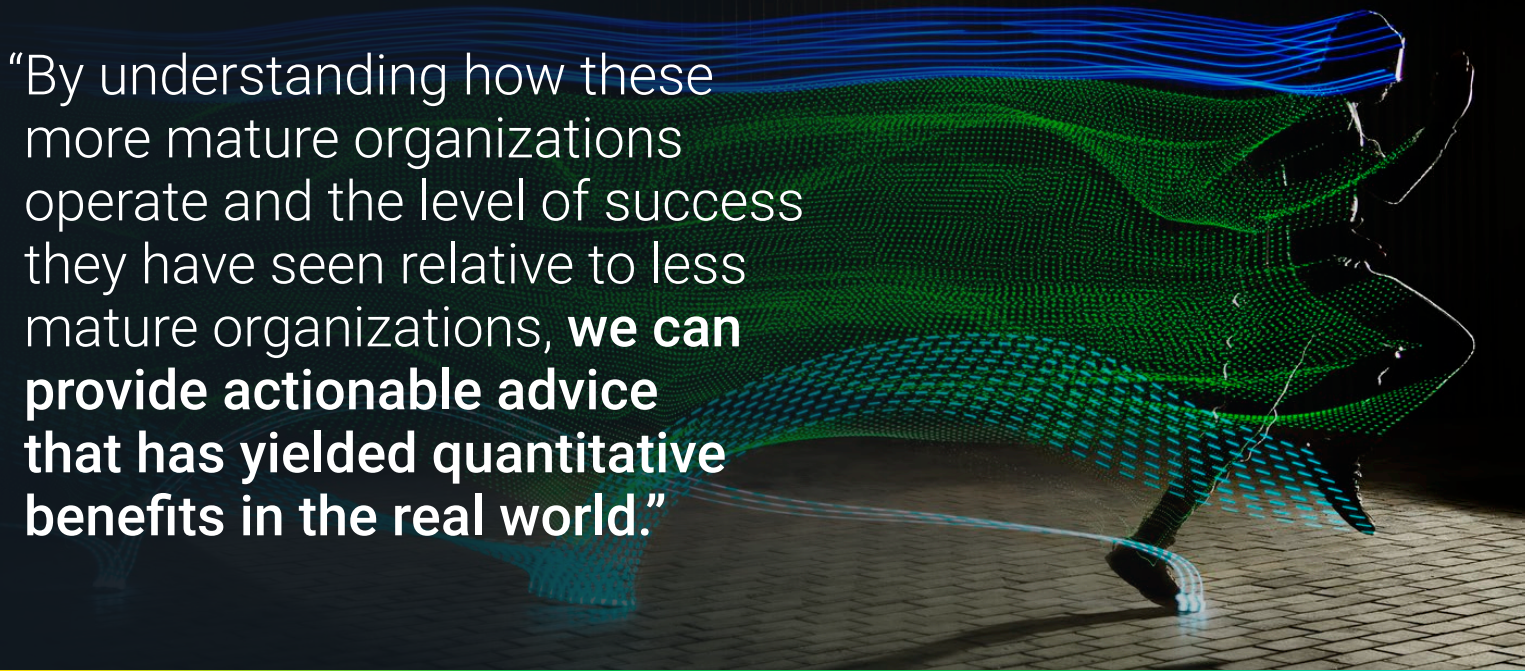
infoblox

This Enterprise Strategy Group eBook was commissioned by Infoblox and is distributed under license from TechTarget, Inc.

© 2024 TechTarget, Inc. All Rights Reserved.

Contents

Foreword	3
Executive Summary	4
• Key Findings	4
• The Four Common Denominators of Hybrid, Multi-cloud Success	5
Introduction	6
• Establishing a Method to Assess an Organization’s Hybrid, Multi-cloud Management Maturity	7
• The Four Tenets of Enterprise Strategy Group’s Hybrid, Multi-cloud Management Maturity Model	7
• Differences Seen in Hybrid, Multi-cloud Management Maturity Across Organizations’ Firmographics	8
A Mature Approach Enables Superior ITOps and SecOps Outcomes	9
• The Direct Technical Impact of Leveraging a Cloud-neutral Tool for Unified DNS, DHCP, IPAM, and Security Solution Decisions for Cloud	9
• Additional Correlations Showing How Big an Impact Improved Maturity Has for Organizations’ IT and Security Outcomes	10
A Mature Approach Supercharges Developer Velocity and Innovation	13
• The Direct Innovation Impact of Making Cloud-neutral DNS, DHCP, IPAM, and Security Solution Decisions	13
• Data Further Validates that Hybrid, Multi-cloud Management Maturity Drives Innovation	13
Learning From the Leaders: What Organizations Should Strive for to Improve Their Maturity	16
• Leading Organizations Adopt Cloud-neutral DDI That Integrates With CSP-provided Tools	16
• Leading Organizations Aggressively Automate NetOps and SecOps in Cloud Environments	17
• Leading Organizations Use the Full Security Potential of DNS	18
• Leading Organizations Are Converging Tools in Use Across NetOps and SecOps	19
About Infoblox	20
Appendix I: Research Methodology and Respondent Demographics	21
Appendix II: Criteria for Evaluating Organizations’ Maturity	22



“By understanding how these more mature organizations operate and the level of success they have seen relative to less mature organizations, **we can provide actionable advice that has yielded quantitative benefits in the real world.**”

Foreword

Modern business moves at a lightning-fast pace. Identifying a market need, building a product to address it, and quickly presenting it to customers distinguishes innovators from followers. In today's highly digitized environment, technology serves as a core enabler of the business. Ultimately, the need to support the business is a driving force that motivates cloud migration and infrastructure modernization.

All of this is to say that these initiatives are clearly strategic and not new, as we are now approaching the two-decade mark of the cloud computing era. Yet, many organizations continue to struggle, especially as the need to better integrate cloud and on-premises infrastructure becomes more acute. There is no single fix to solve this, but rather, organizations must determine aspects across people, processes, and technology that will have the greatest impact in generating the best positive outcomes for the business.

Ultimately, that was the goal of this research: to identify enterprises that have knowingly—or not—found the keys for successfully managing hybrid, multi-cloud environments. By understanding how these more mature organizations operate and the level of success they have seen relative to less mature organizations, we can provide actionable advice that has yielded quantitative benefits in the real world. Organizations that are able to learn from these leaders can accelerate the optimization of their hybrid, multi-cloud strategy and put the business in a better position to succeed in a highly dynamic and competitive business environment.



John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

Executive Summary

Few technologies could be argued to be more transformational to business operations today than cloud computing and the solutions used to secure cloud environments. However, determining the optimal strategy for operating and securing a hybrid, multi-cloud environment presents many challenges. The complexity inherent in managing multiple cloud providers with varying architectures, services, and pricing models can be overwhelming. Additionally, ensuring consistent performance and reliability across different clouds while minimizing costs and avoiding vendor lock-in is difficult work for overburdened IT teams. Compounding matters, IT teams must also continuously modernize their on-premises IT infrastructure, either because not all workloads are suitable candidates for public cloud environments or because the effort to refactor them for the public cloud doesn't offer a compelling return on investment. Finally, IT teams are under pressure to optimize developer experiences. Developers are crucial for competitive differentiation. Their needs include a seamless development experience, flexible deployment options, and robust tooling for monitoring, debugging, and security.

This report, and the research that underpins it, seeks to illuminate the right approach to hybrid, multi-cloud operations so that decision-makers can give their organizations the best chance to compete and win in their markets. It does so not by outlining a vendor or analyst's opinion but by examining the data provided by 1,000 IT decision-makers and influencers knowledgeable about the organization's public cloud environment (see *Appendix I: Research Methodology and Respondent Demographics* for more details).

The results show if, and by how much, the decisions organizations make about the structure of network and security teams—and the tools they use—affect a wide variety of ITOps, SecOps, and business outcomes. Organizations can use this research as a guide to improve their own cloud operations.

Key Findings

How are mature cloud organizations leading the way?



They have better cross-cloud visibility. They are 2.1 times more likely than their peers to say their approach to cloud networking and security has enabled significantly better cross-cloud visibility and 66% more likely to say it has significantly reduced risk.



They see 23% larger cloud cost reductions. Cost optimizations in cloud networking and security technologies drive their savings.



They experience greater application resilience. 56% say they've seen one or fewer business-critical cloud outages in the past year (versus 37% of their peers who reported the same thing), and they are 3.8 times as likely to say they can restore cloud services in minutes.



They excel in security investigations and activity detection. They are 2.5 times more likely to have significantly accelerated security investigations and 2.3 times more likely to have significantly accelerated the detection of suspicious activities.



They exceed end-user satisfaction goals. These organizations are 2.3 times more likely to beat satisfaction goals and 3.6 times more likely to be confident in their cloud reporting capabilities. Additionally, 76% of respondents report their technical teams are under pressure to increase cloud agility to accelerate developer velocity.

How do mature organizations excel in developer enablement and innovation?



They increase profitability and accelerate cloud deployments. Leading IT organizations are 3.6 times more likely to achieve both through better cloud asset management.



They delight developers. They are 3 times more likely to be viewed as competitive differentiators by developers.



They accelerate developer agility. These organizations 4.6 times as likely to enable on-demand code deployment.



They gain a competitive edge in time to market. They are 4.2 times more likely to outpace competitors or bring more products to market.



They delight customers. They are 2.2 times more likely to exceed customer satisfaction scores for cloud-hosted applications.

The Four Common Denominators of Hybrid, Multi-cloud Success

The research shows there are four characteristics that most mature hybrid, multi-cloud managers share and that every organization should pattern themselves after to optimize their outcomes. Mature organizations do the following:

1. Converge network, security, and cloud operations practitioners into a cloud operations center of excellence.

88%

of the most mature organizations have increased the frequency with which these teams meet and collaborate.

85%

have taken steps to align the goals and KPIs these teams strive to achieve.

81%

have created a formal cloud center of excellence with representation from both networking and security practitioners.

2. Employ cloud-neutral network and security tools.



97%

of the most mature organizations leverage cloud-neutral domain name system (DNS), dynamic host configuration protocol (DHCP), and IP address management (IPAM) solutions, as opposed to only using solutions provided by cloud service providers (CSPs).



97%

leverage third-party security tools as opposed to just security features provided by cloud operators. This approach enables organizations to create cross-cloud integrations with their tool sets, helping drive more complete visibility and reducing the need for cloud provider-specific expertise among staff.

3. Embrace DNS as a highly valuable cloud security solution.

78%

of the most mature organizations use DNS extensively in security incident investigations.

77%

do so to detect and block malware.

75%

do so as a data loss prevention (DLP) mechanism.

i In all cases, mature organizations report greater reliance on DNS.

4. Enable automation holistically in cloud operations, spanning both network and security workflows.



Modern, dynamic cloud environments require CloudOps to be highly automated in order for teams to keep pace. Mature organizations are further along in instrumenting this automation in areas like resource provisioning, anomaly detection, asset discovery, and audit reporting.

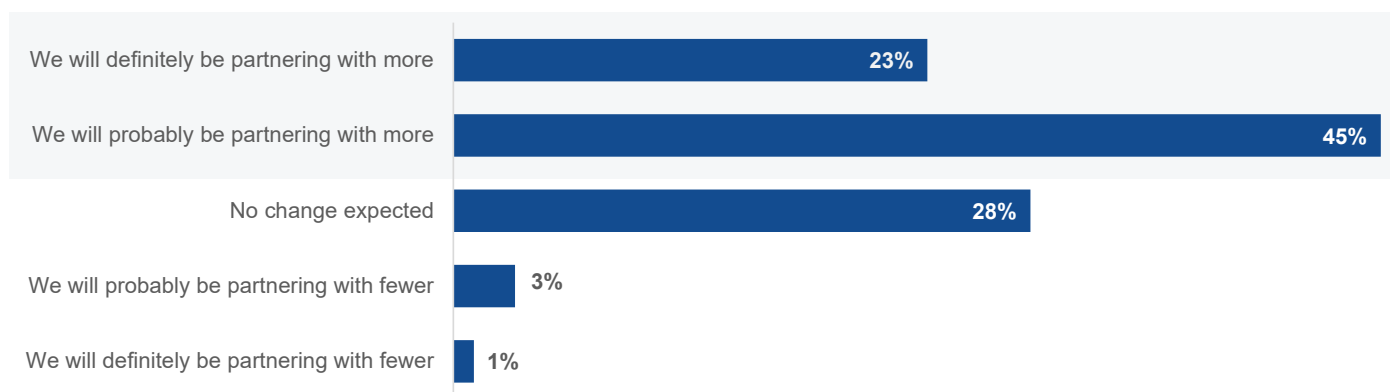
Introduction

The central thesis of this research is that there are specific, actionable steps every organization can employ to improve their hybrid, multi-cloud operations and associated business outcomes. This is critical for organizations to understand as hybrid, multi-cloud operating models are not only mainstream, but they will also endure at organizations for the foreseeable future.

The research asked respondents to agree or disagree that there are workloads and data on premises today that are not candidates to run on public cloud infrastructure due to control or sensitivity considerations, and 73% of respondents agreed this was the case for their organization. Similarly, respondents were asked if there were on-premises workloads that were so stable or unchanging that the effort of refactoring them for the public cloud was not a compelling use of time or resources, and 72% agreed. In short, the vast majority of organizations that partner with multiple public cloud providers today still see a need to maintain an on-premises IT infrastructure footprint.

The research also indicates that 91% of organizations are already operating in a multi-cloud mode today. All of the 1,000 organizations represented in the sample already currently partner with multiple public cloud IaaS providers. However, in the course of seeking these organizations to participate in the research, only 9% of respondents starting the survey said their organization partnered with a single public cloud IaaS provider or did not leverage public cloud IaaS; these were omitted from the final sample. Among those organizations already partnering with multiple public cloud IaaS providers, the vast majority (68%) expect to partner with even more 12 months from now (see Figure 1).

Figure 1. Multi-cloud Organizations Will Work With Even More IaaS Providers Over Time (Percent of respondents, N=1,000)



While leveraging multiple public clouds brings with it advantages, it also introduces challenges. For example:



73%

of respondents reported that their organization had encountered skills gaps as a direct result of using multiple cloud providers and leveraging management tools exclusive to those environments.



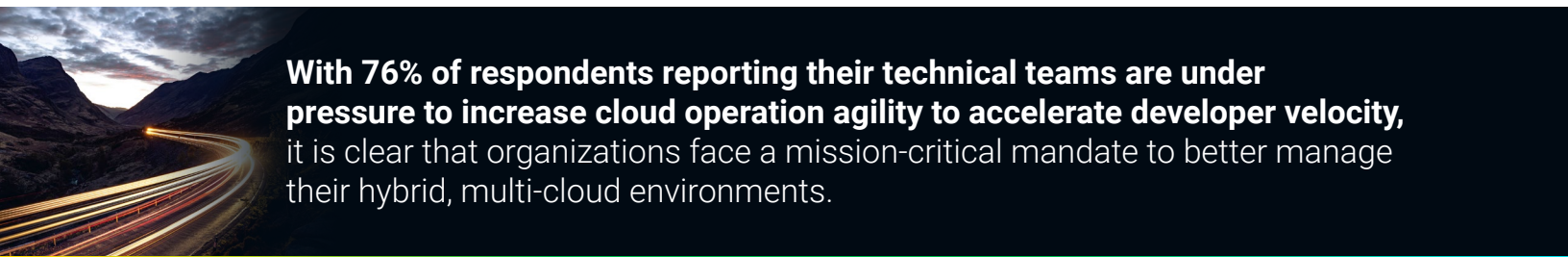
65%

said this same dynamic in their environment had led to inefficiencies and delays in their cloud operations.



63%

said this multi-cloud fragmentation had actually resulted in incidents (e.g., downtime, security issues) tied to administrator errors.



With 76% of respondents reporting their technical teams are under pressure to increase cloud operation agility to accelerate developer velocity, it is clear that organizations face a mission-critical mandate to better manage their hybrid, multi-cloud environments.

Establishing a Method to Assess an Organization's Hybrid, Multi-cloud Management Maturity

While the survey included a total of 50 questions, TechTarget's Enterprise Strategy Group used 11 of those questions as the determining factors in a maturity model to segment and compare organizations based on their hybrid, multi-cloud management capabilities. Based on the answers to these questions, respondents' organizations could earn between 0 and 105 total maturity points, with a greater score indicating a higher maturity level. *Leading* organizations were defined as those organizations earning more than 80 maturity points, *Converging* organizations as those that earned between 70.25 and 80 points, *Emerging* organizations as those that earned between 60 and 70 points, and *Nascent* organizations as those that earned fewer than 60 points (see *Appendix II: Criteria for Evaluating Organizations' Hybrid, Multi-cloud Maturity* for more details).

The Four Tenets of Enterprise Strategy Group's Hybrid, Multi-cloud Management Maturity Model

1. Organizations should establish a cross-functional cloud platform team that combines network, security, and cloud operations practitioners.



Converging network and security to be part of an organization's cloud operations center of excellence can yield significant benefits in terms of efficiency, agility, and security. By breaking down traditional silos between these two teams, the organization can foster better collaboration and alignment of goals, leading to streamlined processes and faster decision-making. In the context of the maturity model, questions to assess an organization's progress include specific steps taken to converge teams, like creating hybrid roles that span these disciplines or increasing the frequency of collaboration, the propensity of the organization to have deployed common tools used in both of these teams, and the establishment of a cross-functional cloud or platform engineering team focused on meeting the organization's requirements for scalability, reliability, security, and performance in cloud environments.

2. Organizations should be using enterprise-grade, cloud-neutral networking solutions.



These solutions, such as third-party-provided DNS, DHCP, and IPAM (DDI), provide robust management capabilities, enabling efficient provisioning, allocation, and tracking of network resources in dynamic cloud environments. By leveraging tools that are designed for multi-cloud operations, as opposed to CSP-provided tools that only work on a single provider's infrastructure, organizations can enhance cross-cloud consistency and attain greater agility, reliability, and performance. The centralized management and reporting capabilities provided by these solutions enable better visibility and control over network infrastructure, simplifying compliance efforts and reducing operational overhead.

3. Organizations should take a defense-in-depth approach to security solutions, including using DNS for a broad range of security use cases.

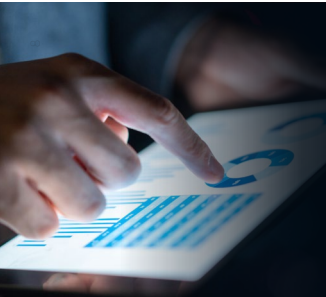


The maturity model advocates for an organization not to be solely reliant on the cloud security and monitoring tools provided by IaaS providers. This is because every organization has different specific security policies, regulatory obligations, and/or governance standards that may require additional security measures beyond what cloud providers offer. In particular, the use of DNS across a spectrum of security use cases—like enforcing acceptable use policies, detecting and blocking malware, and incident investigation or threat hunting—is an organizational attribute rewarded in the maturity model.

4. Organizations should strive to automate both NetOps and SecOps workflows in the cloud.



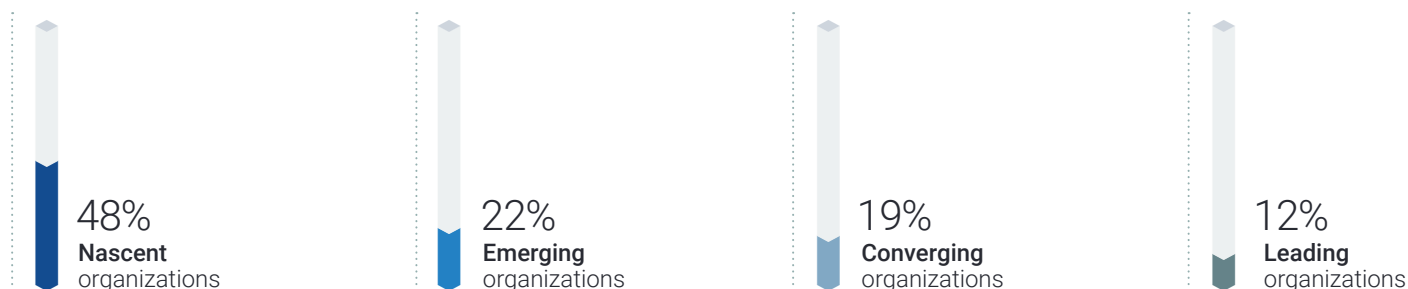
Automation increases operational efficiency by reducing manual effort and human error, enabling organizations to deploy, manage, and scale network infrastructure and security services more quickly and consistently. This agility enables faster response to changing business requirements and security threats and also improves productivity, both within technical teams and for stakeholders like developers.



88% of the market today has meaningful room to improve their adherence to the tenets in Enterprise Strategy Group's maturity model.

As shown in Figure 2, a mere 12% of organizations represented in the survey earned enough maturity points to achieve Leader status, meaning that 88% of the market today has meaningful room to improve their adherence to the tenets in Enterprise Strategy Group's maturity model. Conversely, the plurality of organizations were segmented as Nascent organizations, with the most room for improvement but also standing to gain the most from that improvement.

Figure 2. The Distribution of Organizations, by Hybrid, Multi-cloud Management Maturity Level (Percent of organizations represented, N=1,000)



Differences Seen in Hybrid, Multi-cloud Management Maturity Across Organizations' Firmographics

As it relates to hybrid, multi-cloud management maturity across geographic regions, those in Western Europe tend to trail, with 55% falling into the Nascent market segment versus 51% of organizations in the Asia-Pacific region and 40% of organizations in North America. Conversely, those in North America more often attained a Converging or Leading rating (34%) relative to their Asian (29%) and European (27%) counterparts.

From a company size perspective, midsize enterprises (i.e., those with 5,000 to 9,999 employees) tend to be struggling most, with 53% falling into the Nascent category versus 48% of small enterprises (i.e., those with 1,000 to 4,999 employees) and 42% of large enterprises (i.e., those with 10,000+ employees).

Inspecting the data by vertical sector shows, somewhat surprisingly, that healthcare and life sciences organizations are the furthest along, with 19% attaining Leader status and another 34% achieving Converging status. Sectors like business services and financial services graded out around the mean, while manufacturers, communications and media companies, and retailers tended to lag the aggregate market.

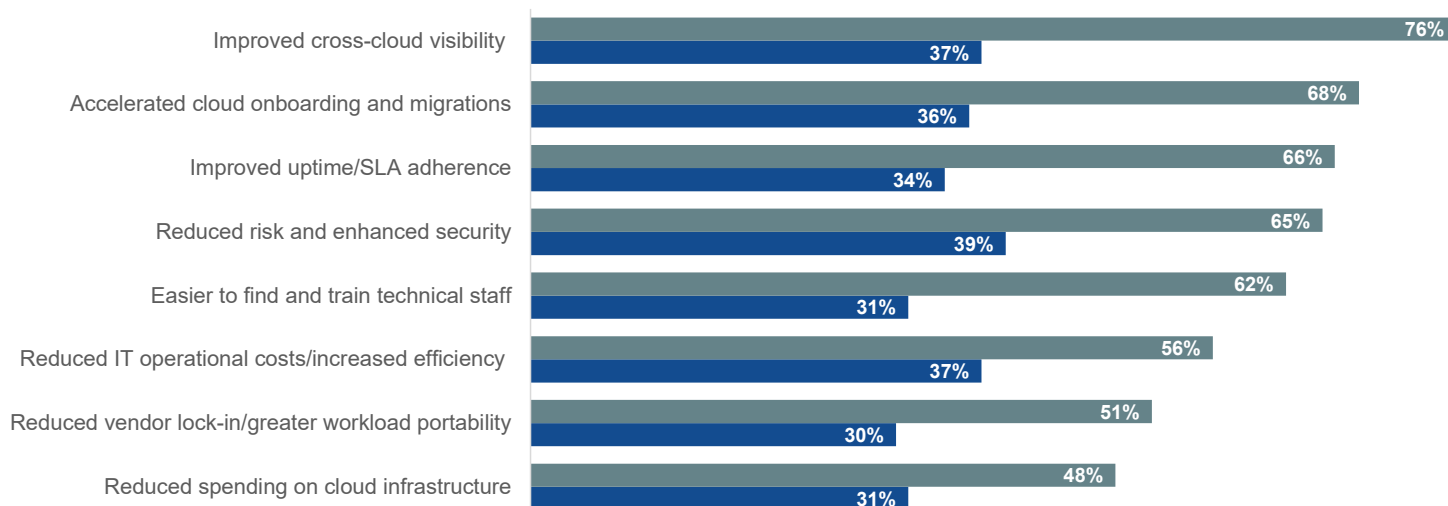
A Mature Approach Enables Superior ITOps and SecOps Outcomes

The Direct Technical Impact of Leveraging a Cloud-neutral Tool for Unified DNS, DHCP, IPAM, and Security Solution Decisions for Cloud

A core question addressed in the research was, “Does a causal link between hybrid, multi-cloud management maturity and improving technical CloudOps outcomes exist?” The answer was a resounding “yes.” As noted, the maturity model specifies distinct actions organizations should take with respect to cloud networking and security technologies (e.g., leverage tools from third parties in addition to cloud providers’ tools, deploy common tools across security and networking staff, etc.). Leading organizations employ these techniques, while their less mature peers do not. Next, a foundational question was asked of respondents: Is your organization’s approach to cloud networking and security technologies materially improving ITOps and SecOps outcomes in the cloud? Respondents could answer with a range of responses, from “yes, significantly” to “not at all.” The data shows that a more mature approach to cloud networking and security solutions drives a greater impact (see Figure 3).

Figure 3. The Degree to Which Cloud Networking and Security Solutions Are Enabling Improved Technical Cloud Outcomes, by Organizations’ Maturity Level (Percent of respondents saying “Significantly”)

■ Leading organizations ■ Nascent organizations



Respondents at Leading organizations were much more apt than those at Nascent organizations to say their cloud networking and security solution decisions have been played a significant role in the organization’s achievements of positive cloud outcomes.

This includes being:

2.1x MORE LIKELY

to have enabled significantly better cross-cloud visibility (76% versus 37%).

2x MORE LIKELY

to have eased recruitment and retention challenges on technical teams (62% versus 31%).

NEARLY TWICE AS LIKELY

to have significantly improved uptime (66% versus 34%).

66% MORE LIKELY

to have significantly reduced risk (65% versus 39%).

Additional Correlations Showing How Big an Impact Improved Maturity Has for Organizations' IT and Security Outcomes

Beyond this direct validation that cloud neutral implementations of DNS, DHCP, IPAM, and security solutions are improving cloud outcomes, the data enables us to further examine how wide the gap between Leaders and their less mature peers is.

Lowering Cloud Costs

As it relates to cloud costs, we saw that 48% of Leading organizations feel their network and security solutions are helping them to optimize their cloud costs, versus 31% of Nascent organizations. This is likely as a result of Leaders' improved cross-cloud visibility, which enables better asset management and prevents scenarios where orphaned cloud infrastructure can cause surprise cloud costs. Additionally, the greater flexibility organizations have to choose the right cloud for the right workload via reduced lock-in likely helps many of these organizations reduce their cloud costs.

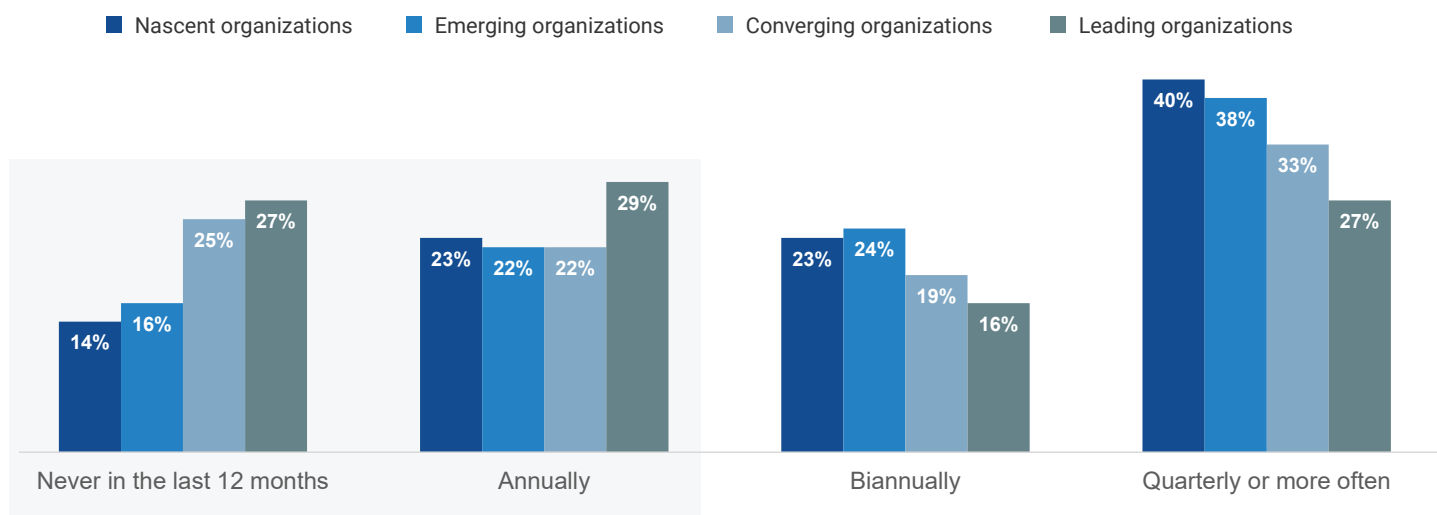
The research further explored this concept by asking respondents to quantify how much network and security solutions had reduced their cloud costs, relative to if those technologies were not in place. In the aggregate, Leading organizations estimated a 23% larger cost reduction than their Nascent peers (a 22.1% mean reduction versus a 17.9% mean reduction, respectively).

Ensuring Continuity of Cloud Applications and Services

We also saw that 66% of Leading organizations feel their network and security solutions are helping them improve cloud resilience, versus 34% of Nascent organizations. The research further shows just how much more reliable Leaders' environments are: When asked how often in the past 12 months any cloud-hosted, business-critical workload encountered an outage or instance of severely degraded performance, the majority (56%) of Leaders said this had not occurred or occurred only once. Just 37% of Nascent organizations enjoyed this same level of cloud resilience (see Figure 4).

When outages do occur, the data shows Leading organizations are much faster than their peers both in terms of detection and recovery. When asked how long it takes for cloud teams to detect a problem with workloads they are responsible for, particularly from the time the performance degradation or outage occurs, 58% of those at Leading organizations said it takes seconds (24%) or minutes (34%). Just 35% of Nascent organizations said they can detect issues with the same speed. When asked about cloud teams' mean time to repair (MTTR), instances of unplanned downtime, or serious degradations, respondents at Leading organizations were 3.8x as likely to say MTTR is measured in minutes as opposed to hours or days (34% versus just 9% of Nascent organizations).

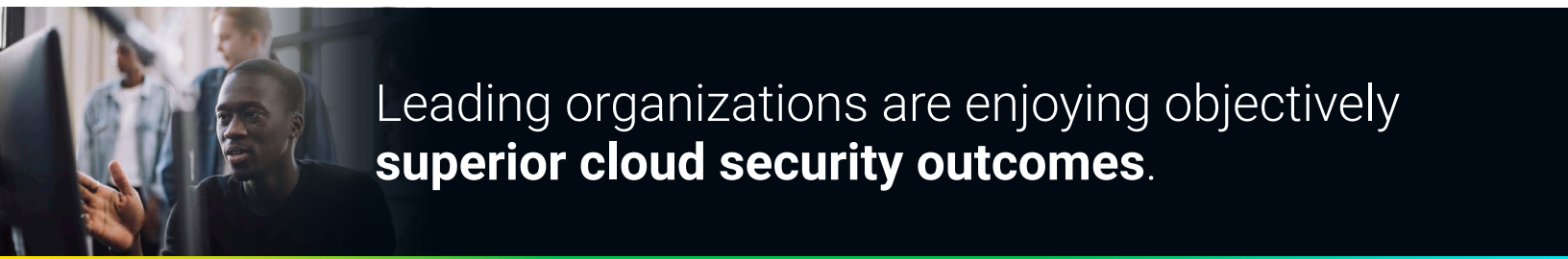
Figure 4. How Often Cloud-hosted, Business-critical Workloads Go Down, by Organizations' Maturity Level
(Percent of respondents at each organization type)



56% of Leaders vs. 37% of Nascent organizations



reported a cloud-hosted, business-critical workload outage or instance of severely degraded performance **had not occurred or occurred only once.**



Leading organizations are enjoying objectively superior cloud security outcomes.

Securing Cloud-hosted Workloads and Accelerating Threat Detection and Response

As noted previously, 65% of Leading organizations feel their network and security solutions are helping them significantly reduce cloud risk, versus 35% of Nascent organizations. Going deeper, we see Leading organizations are enjoying objectively superior cloud security outcomes. In the same way respondents were questioned about cloud outages, they were also asked how many times in the past 12 months any cloud-hosted, business-critical workload had been successfully compromised by a bad actor. Once again, the majority (62%) of respondents at Leading organizations said this had not occurred or occurred only once, while far fewer (44%) of Nascent organizations had achieved the same level of cloud security.

The survey also explored trends in SecOps agility. Respondents were asked how the time cloud security teams need to detect suspicious activity in the cloud, investigate it, and respond to threats had changed over the past 12 months. In all cases, Leading organizations were much more likely than their Nascent peers to say each of these SecOps workflows had significantly accelerated (see Figure 5).

Specifically, over the past 12 months, Leaders were:

2.3x MORE LIKELY

to have significantly accelerated the detection of suspicious activity.

2.5x MORE LIKELY

to have significantly accelerated security investigations.

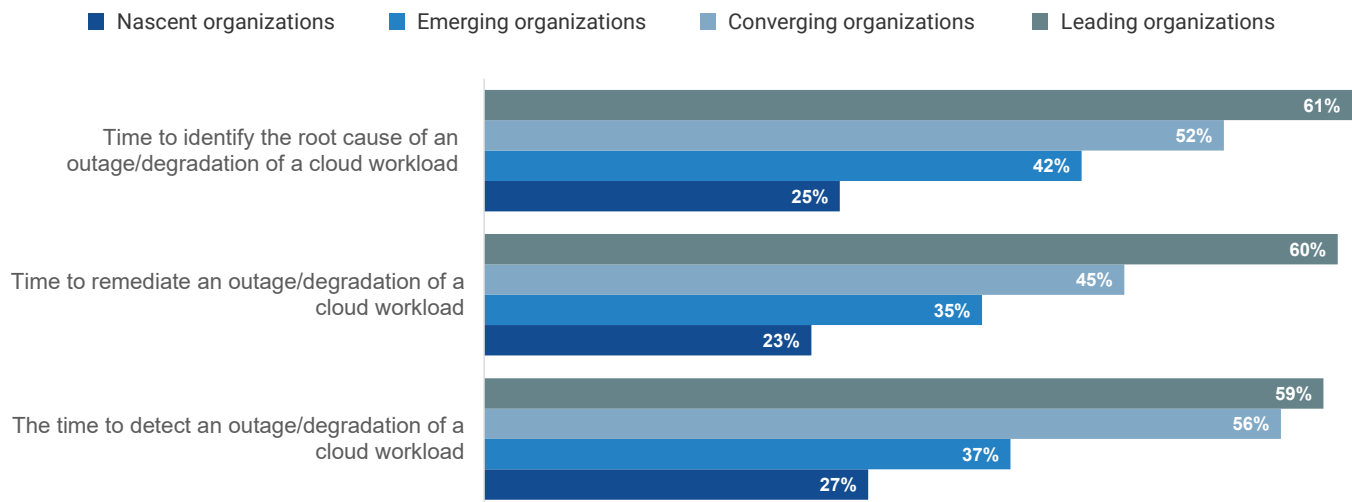
2.2x MORE LIKELY


to have significantly accelerated incident response.

Data supports the hypothesis that a more mature approach to hybrid, multi-cloud management, which advocates for the use of a cloud-neutral DNS platform across a broad set of security operations, helps increase security teams' agility in threat detection and response.

Figure 5. Changes in SecOps Agility, by Organizations' Maturity Level

(Percent of respondents saying processes had accelerated "Significantly" in the past 12 months)





Leading organizations are **3.1x as likely to be completely confident in their IT and security teams' ability** to deliver on the requirements of the business as it relates to cloud adoption.

Leaders on Hybrid, Multi-cloud Management Maturity Can Better Support the Business

Ultimately, an IT organization's mission is to effectively leverage technologies to support the business's requirements. In the context of the cloud, this means empowering the business to adopt cloud services that streamline operations, enable scalability, increase organizational agility, and support innovation, all while ensuring data security and compliance. In this regard, Leading organizations have far more confidence as they look ahead as compared with their less mature counterparts: Leading organizations are 3.1x as likely to be completely confident in their IT and security teams' ability to deliver on the requirements of the business as it relates to cloud adoption (59% versus 19%, see Figure 6).

Figure 6. IT's Confidence in its Ability to Deliver on the Business's Cloud Requirements, by Organizations' Maturity Level

(Percent of respondents at each organization type)

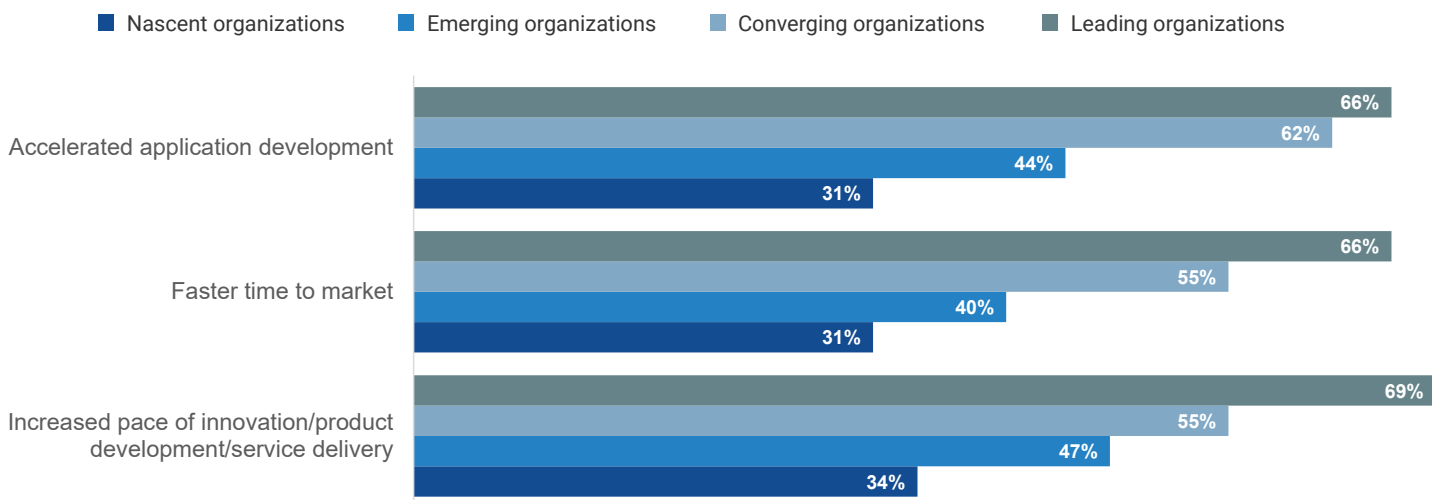


A Mature Approach Supercharges Developer Velocity and Innovation

The Direct Innovation Impact of Making Cloud-neutral DNS, DHCP, IPAM, and Security Solution Decisions

Moving beyond technical outcomes, the research also sought to validate that a mature approach to hybrid, multi-cloud management helps improve organizational agility and innovation. Once again, the data strongly supports this thesis. Respondents were asked if their organization's approach to cloud networking and security technologies is materially improving several application development and innovation-in-the-cloud outcomes. Respondents could answer with a range of responses, from "yes, significantly" to "not at all." The data shows that a more mature approach to cloud networking and security solutions that emphasizes automation and the adoption of third-party, cloud-neutral DDI drives a greater impact (see Figure 7).

Figure 7. The Degree to Which Cloud Networking and Security Solutions Are Enabling Improved Innovation Outcomes, by Organizations' Maturity Level
(Percent of respondents saying "Significantly")



Respondents at Leading organizations were much more apt than those at Nascent organizations to say their cloud networking and security solution decisions have been playing a crucial role in the organization's achievement of positive innovation outcomes. This includes being:

2.1x MORE LIKELY

to have enabled significantly faster application development (66% versus 31%).

2.1x MORE LIKELY

to have significantly accelerated time to market (66% versus 31%).

2.1x MORE LIKELY

to have significantly increased their pace of overall innovation (69% versus 34%).

Data Further Validates that Hybrid, Multi-cloud Management Maturity Drives Innovation

Clearly, respondents at Leading organizations feel that the cloud networking and security decisions their organizations are making are helping them operate in a more agile and innovative manner. The data backs up this sentiment, with objective measures showing how much better Leading organizations are performing.

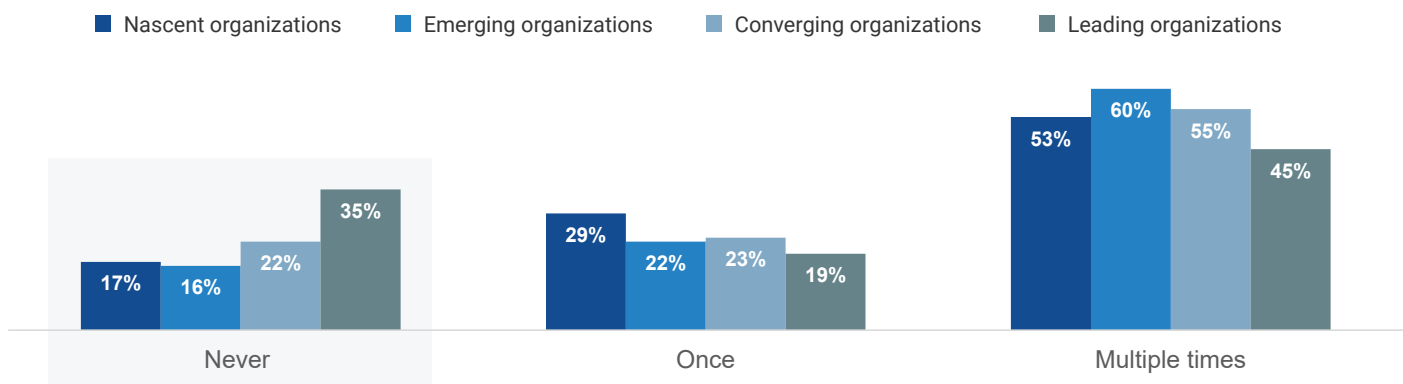
Leading organizations were found to substantially reduce application development friction relative to their peers.

Leaders on Hybrid, Multi-cloud Management Maturity Better Enable Application Developers

The concepts of *developer enablement* and *development velocity* were touched on in several areas of the research, and, in all cases, organizations with greater cloud maturity reported superior results.

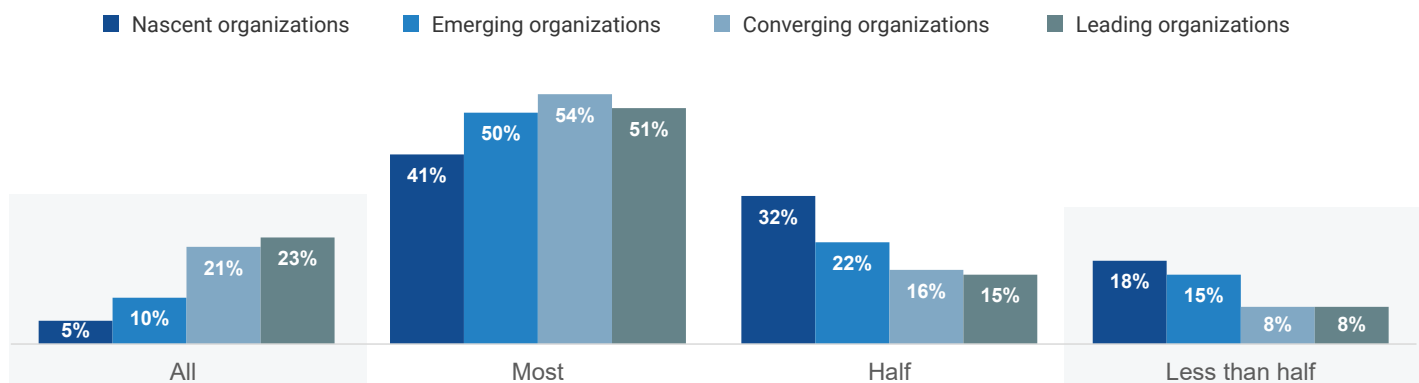
First, the idea of IT and security teams being roadblocks for development teams was investigated. The survey asked respondents how often application development projects had been delayed in the prior 12 months due to the IT or security team's need for more time to inspect cloud services that underpin the project. Leading organizations were found to substantially reduce application development friction relative to their peers. Specifically, respondents at Leading organizations were 2.1x as likely to say IT and security hadn't delayed any development projects in the last year, while the majority of all other maturity cohorts report this has happened multiple times (see Figure 8).

Figure 8. The Number of Times Annually Application Development Projects Are Delayed by IT and Security Concerns With Cloud Services in Use, by Organizations' Maturity Level (Percent of respondents at each organization type)



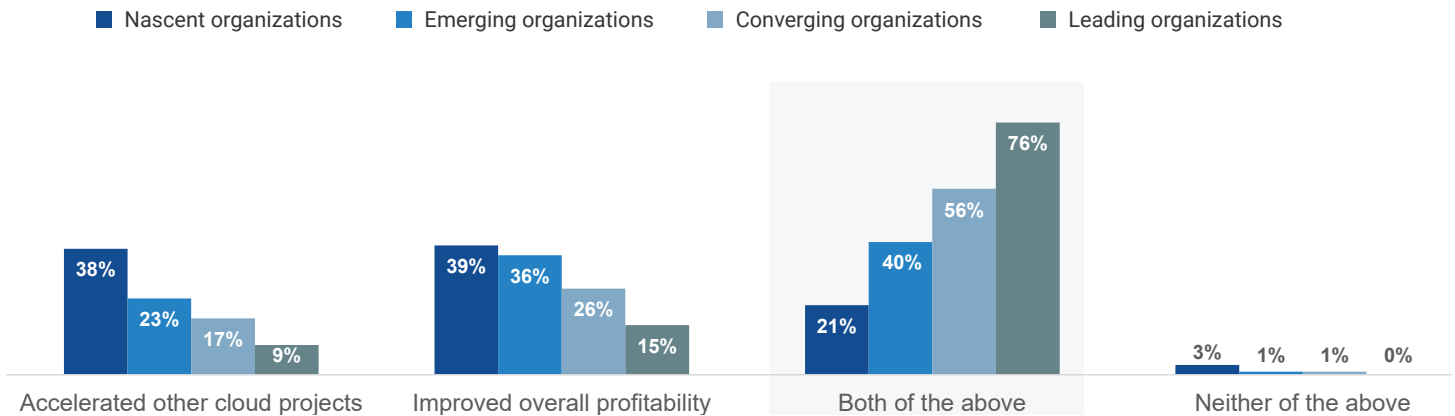
Next, the concept of on-demand code deployment was discussed. The survey asked respondents to consider all their internally developed applications and estimate the proportion for which code is pushed to production "on demand." Leading organizations were found to enable faster developer velocity. Specifically, respondents at Leading organizations were 4.6x as likely as those at Nascent organizations to say they can push code on demand for all their apps, and nearly three-quarters (74%) said they can for at least "most" of their apps (see Figure 9).

Figure 9. Proportion of Applications for Which Organizations Have the Ability to Push Code to Production on Demand, by Organizations' Maturity Level (Percent of respondents at each organization type)



The final aspect of developer enablement discussed ties back to the concept of IT teams being better able to discover and deprovision orphaned cloud infrastructure. Not only does this capability reduce an organization's attack surface, but it ensures an organization is actually able to take advantage of a key cloud value proposition: to only pay for infrastructure it uses. We know from the data that Leading organizations have greater cloud visibility, but the question is, "Does this translate to a bigger business impact tied to limiting wastage in cloud environments?" When asked, respondents at Leading organizations were 3.6x as likely to say they've been able to both accelerate other cloud projects and increase profitability as a result of their ability to discover and deprovision orphaned cloud architecture (see Figure 10). The implication is clear: More hybrid, multi-cloud management maturity results in better visibility into dynamic cloud environments, leading to greater cost savings, which enable the organization to better innovate and improve profitability.

Figure 10. The Business Impact of Discovering and Deprovisioning Orphaned Cloud Infrastructure, by Organizations' Maturity Level
(Percent of respondents at each organization type)

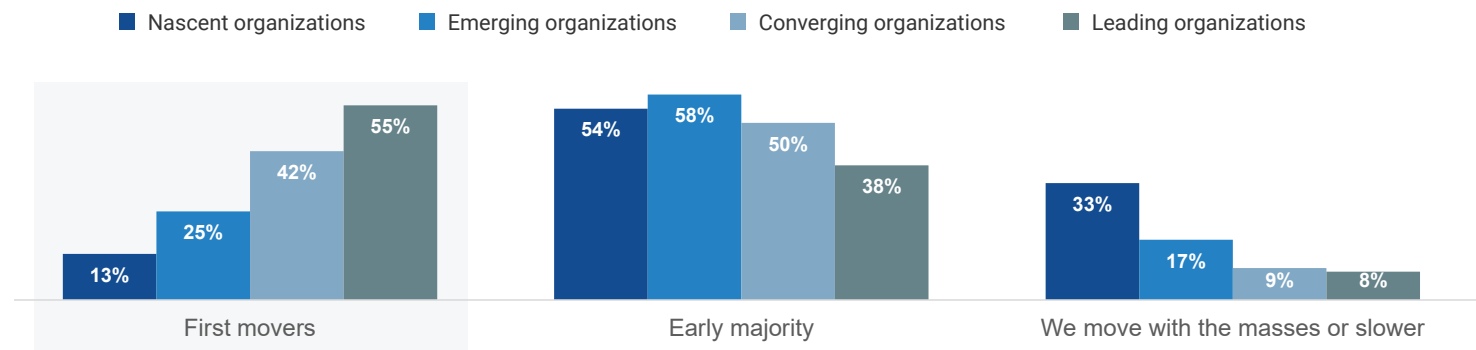


Leaders on Hybrid, Multi-cloud Management Maturity Gain a Competitive Edge as a Result

In an encouraging finding, the research indicates development teams at Leading organizations both recognize and appreciate the market-leading level of enablement their cloud teams are providing to them. All respondents were asked how they think their development team views the IT and security teams, from a "competitive differentiator" all the way to a "business inhibitor." Respondents at Leading organizations were 3x more likely to say their development teams see them as a competitive differentiator (39% versus 13%). On the other hand, respondents at Nascent organizations were 2.9x as likely to say their development teams felt their IT teams had significant room to improve (26% versus 9%).

Independent of this data point, all respondents were asked how their organization performs in areas like time to market and the number of new products developed over time, like new digital services and customer-facing applications. Here again, Leading organizations outperformed the pack. They were over 4x as likely to be first movers in their markets (55% versus 13%, see Figure 11), while Nascent organizations were far more likely to report their organization moves with the masses or is typically behind their competition. This finding, perhaps more than any other, shows the business criticality of an organization improving its hybrid, multi-cloud management maturity. In today's digital-first economy, nearly all companies are technology companies to some degree, and failing to maximize developer enablement may have existential implications for many organizations.

Figure 11. Organizations' Innovation Performance, by Maturity Level (Percent of respondents at each organization type)



Learning From the Leaders: What Organizations Should Strive for to Improve Their Maturity



It's clear that organizations have a lot to gain by increasing their level of hybrid, multi-cloud management maturity. The benefits span IT operations and efficiency, SecOps effectiveness, reduced organizational risk, innovation, and digital transformation. Beyond validating these benefits, the research provides us with insights about the fundamentally different ways Leaders operate, both in terms of technologies in use and how teams function. All organizations should evaluate and seek alignment with these findings.

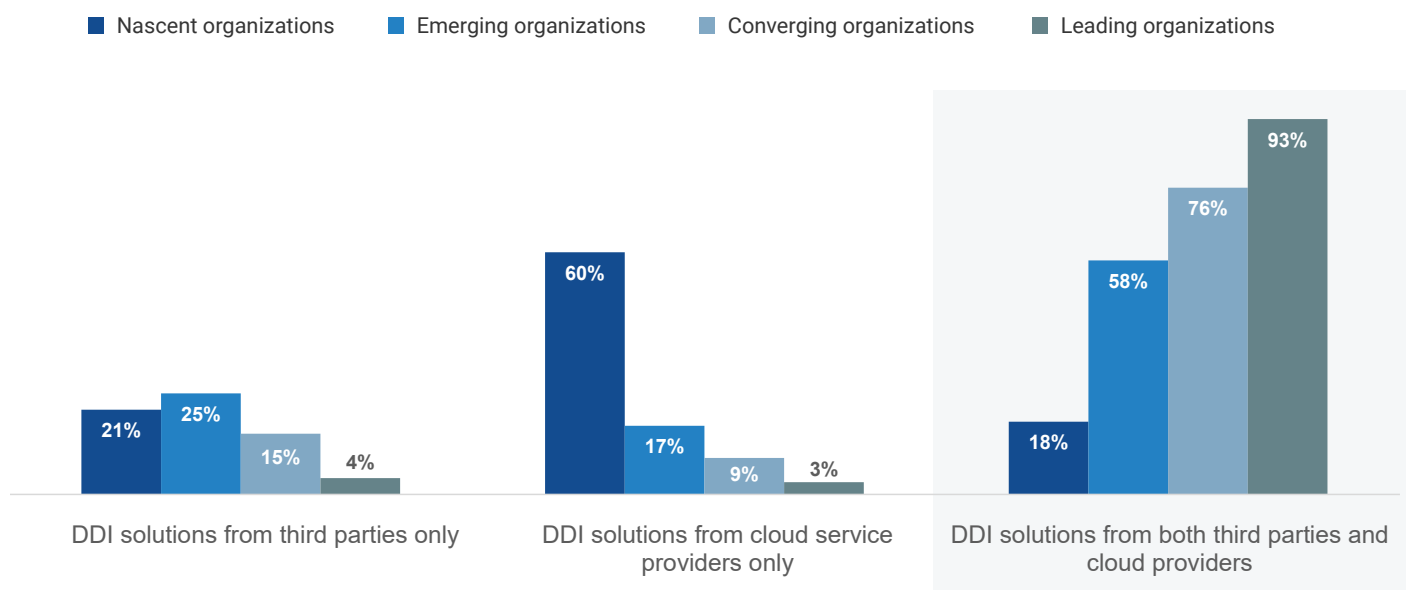
Leading Organizations Adopt Cloud-neutral DDI That Integrates With CSP-provided Tools

Employing cloud-neutral DDI and security tools provides several advantages over using only CSP-provided tools, which are limited in their function to that CSP's infrastructure. These solutions can span clouds and offer the opportunity to achieve a centralized visibility and management plane for networking and security across all clouds in use. This simplifies operations, reduces complexity, and helps eliminate the skill gaps that arise when staff need to learn the capabilities and services of each cloud provider.

The data shows just how ubiquitously Leading organizations leverage cloud-neutral, third-party DDI solutions, with 93% reporting they use solutions from both CSPs and third-party software vendors (see Figure 12). Furthermore, when respondents were asked what DDI solutions they were most reliant on in their clouds, the majority (56%) of those at Leading organizations said they rely on purpose-built, enterprise-grade solutions (versus 23% of Nascent organizations). This data mirrors what was observed in the context of security tools: 89% of respondents at Leading organizations reported their organization uses both cloud-neutral and cloud-provided security management and monitoring tools (versus 14% of Nascent organizations).

Looking at this data through a regional lens, respondents based in North America most often report using cloud-neutral tools alongside cloud-native tools (51% versus 45% of those in Western Europe and 43% of those in Asia), while organizations in Asia were the most likely to be completely reliant on CSP-native tools (41% versus 35% of those in Western Europe and just 29% of those in North America).

Figure 12. Leading Organizations Use Third-party DDI in Their Cloud Environments (Percent of respondents at each organization type)



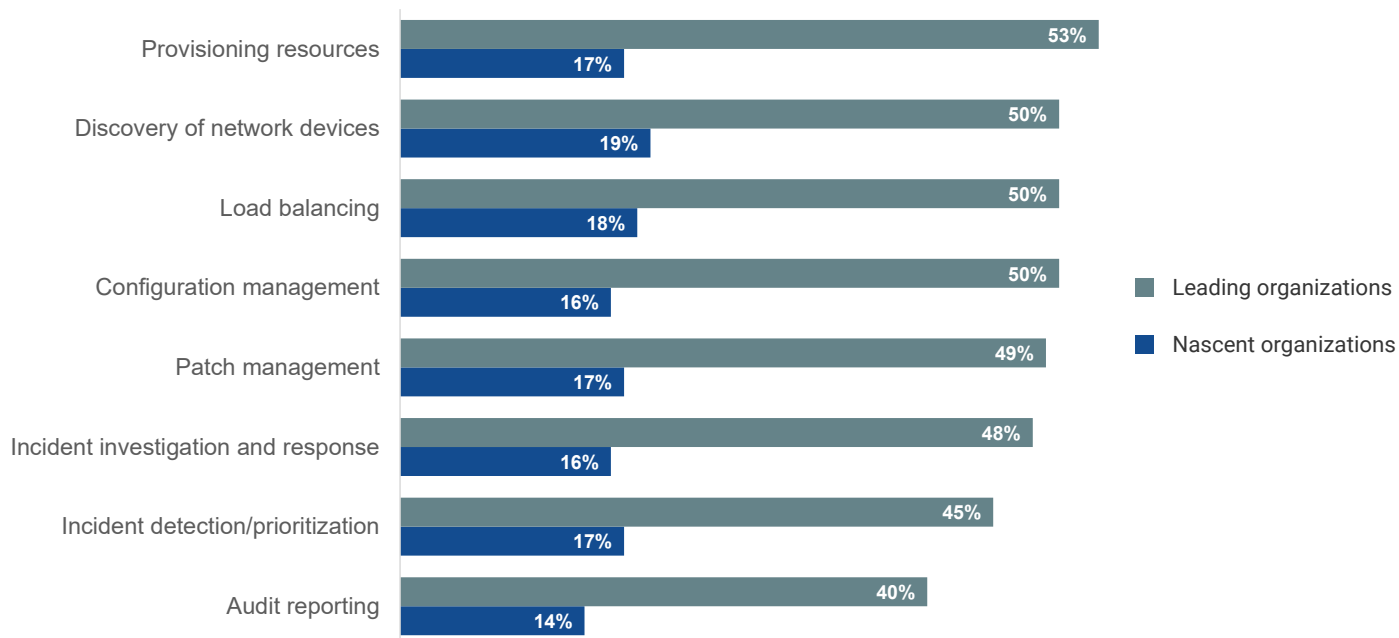
Leading Organizations Aggressively Automate NetOps and SecOps in Cloud Environments

Traditional networks can be manually intensive to manage. As organizations have evolved their environments to include modernized private clouds, connections to multiple public clouds, and hosts of highly dynamic cloud-native applications, the complexity of network operations has compounded. The same dynamics are at play for security operations teams contending with tool sprawl, rapidly expanding attack surfaces, and ever-more sophisticated threats.

To mitigate these trends, Leading organizations have aggressively automated network operations tasks like provisioning resources, discovery of connected devices, load balancing, and more (see Figure 13). In the aggregate, Leading organizations are roughly 3x more likely to have achieved a state of near-complete automation relative to their Nascent peers.

Figure 13. Leading Organizations Highly Automate Many NetOps Workflows

(Percent of respondents saying processes are "Entirely or almost entirely automated")



The story plays out again when respondents were asked to assess the level of automation in security tasks. Respondents at Leading organizations were more likely than those at Nascent organizations to report high levels of automation, including being:

3x MORE LIKELY

to say anomaly detection in the cloud is highly automated (62% versus 21%).

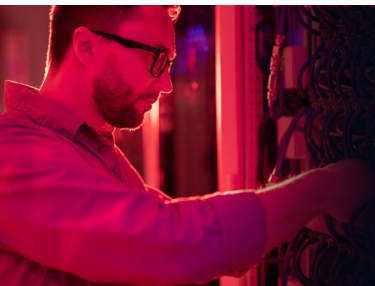
2.9x MORE LIKELY

to say threat intelligence integration across the security ecosystem is highly automated (66% versus 31%).

2.8x MORE LIKELY

to say incident detection and prioritization in their clouds is highly automated (53% versus 19%).

The message is clear: Organizations should seek cloud-neutral DDI and security tools **that offer advanced automation, rich APIs, and many out-of-the-box integrations.**



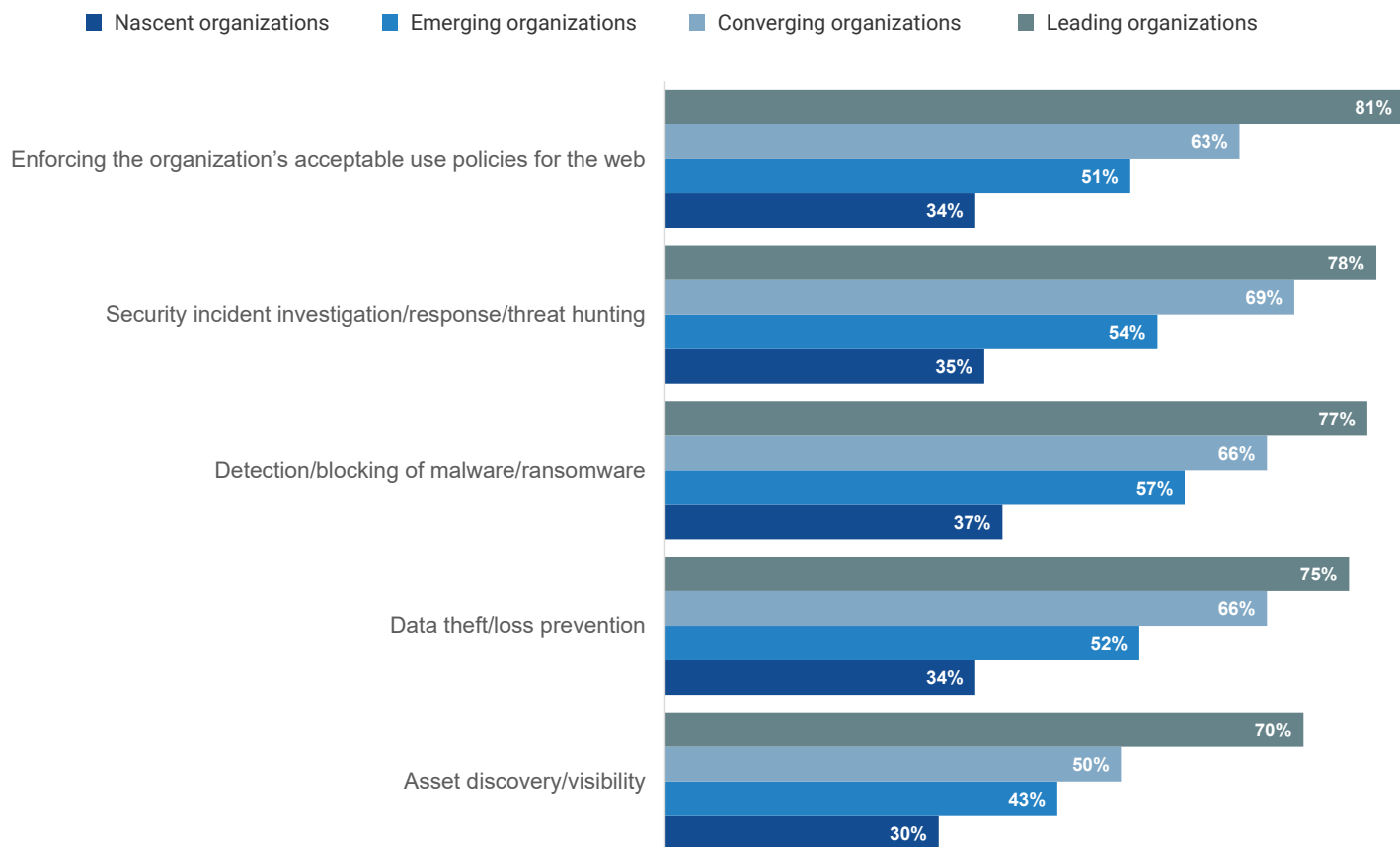
By leveraging DNS for security use cases, organizations **can effectively detect and block malicious activities** at the network perimeter, including malware infections, data exfiltration attempts, and phishing attacks.

Leading Organizations Use the Full Security Potential of DNS

Integrating DNS as a primary security control is a logical cybersecurity strategy due to its potential to thwart a wide array of threats. DNS operates at the foundational level of network communication. By leveraging DNS for security use cases, organizations can effectively detect and block malicious activities at the network perimeter, including malware infections, data exfiltration attempts, and phishing attacks. Additionally, DNS provides valuable insights into network traffic patterns and anomalous behavior, enabling proactive threat hunting and rapid incident response. Leading organizations recognize these opportunities more than their peers. When asked, 70% or more of respondents at Leading organizations reported they use DNS extensively to enforce acceptable use policies (81%), investigate incidents (78%), block malware (77%), and more (see Figure 14).

Looking at this data through a regional lens, respondents based in North America most often report using DNS extensively in security operations, including detecting malware (57% versus 50% of Western European organizations and 46% of those in Asia), preventing data loss (52% versus 49% of Western European organizations and 44% of those in Asia), incident investigation (55% versus 50% of Western European organizations and 44% of those in Asia), and asset discovery (45% versus 37% of Western European organizations and 41% of those in Asia).

Figure 14. Organizations Leverage DNS for Security Use Cases (Percent of respondents saying DNS is “Extensively” used in each use case)





59% report their security and network teams use many of the same solutions to monitor and manage cloud resources, which is **3.1x the rate of Nascent organizations**.

Leading Organizations Are Converging Tools in Use Across NetOps and SecOps

Using common management solutions across both cloud networking and security teams offers organizations several advantages. By sharing common tools, networking and security teams can streamline communication and enhance overall efficiency, as they are able to reference the same data and view it through a common interface. Additionally, leveraging integrated management solutions allows for better visibility and control, enabling more effective monitoring and responses to security incidents and network issues. Finally, utilizing shared solutions can lead to cost savings by eliminating redundant tools. Leading organizations are embracing tool convergence: 59% report their security and network teams use many of the same solutions to monitor and manage cloud resources, which is 3.1x the rate of Nascent organizations (see Figure 15).

Looking at this data from through a regional lens, respondents based in Western Europe most often report their security and networking teams use completely siloed solutions with overlap (26% versus 19% of those based in North America and 16% of those in Asia).

Figure 15. Leading Organizations Are Converging Cloud Management Solutions (Percent of respondents at each organization type)





infoblox[®]

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, Infoblox provides real-time visibility and control over who and what connects to an organization's network so that it runs faster and stops threats earlier.

[LEARN MORE](#)

Appendix I: Research Methodology and Respondent Demographics

To gather data for this report, Infoblox commissioned Enterprise Strategy Group to conduct a comprehensive online survey of 1,000 networking and security decision-makers and influencers knowledgeable about their organization's public cloud environment. Organizations represented span private- and public-sector organizations across the globe, including respondents based in North America (U.S. and Canada), Western Europe (France, Germany, Spain, and the U.K.), and the Asia-Pacific region (Australia, India, Japan, New Zealand, and Singapore). The survey was fielded between December 15, 2023, and January 17, 2024. The margin of error at the 95% confidence level for this sample size is + or - 3 percentage points.

All respondents were offered an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

The following figures detail the demographics and firmographics of the respondent base.

Figure 16. Geographic Distribution of Respondents

(Percent of respondents, N=1,000)

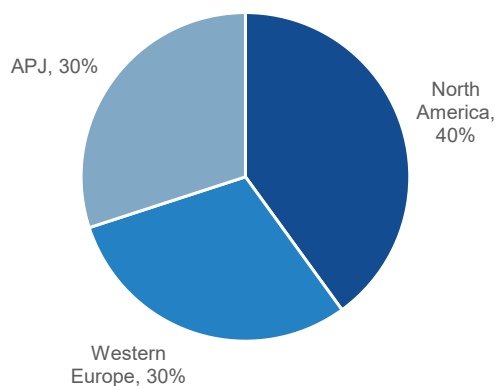


Figure 17. Respondents' Seniority

(Percent of respondents, N=1,000)

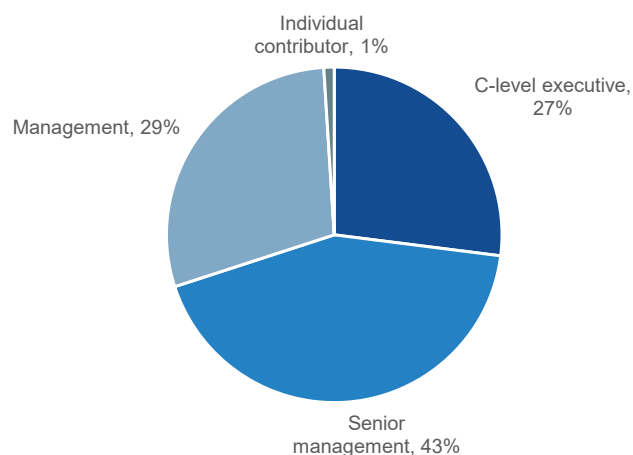


Figure 18. Market Segments Represented

(Percent of respondents, N=1,000)

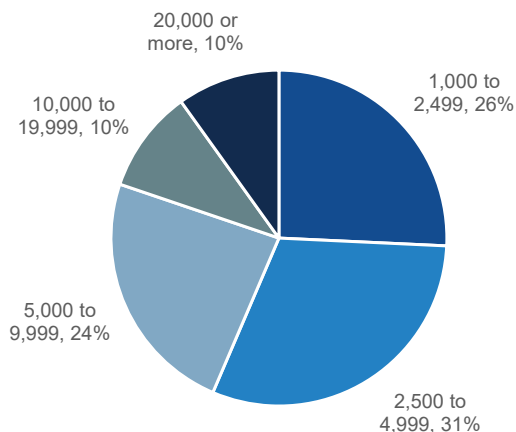
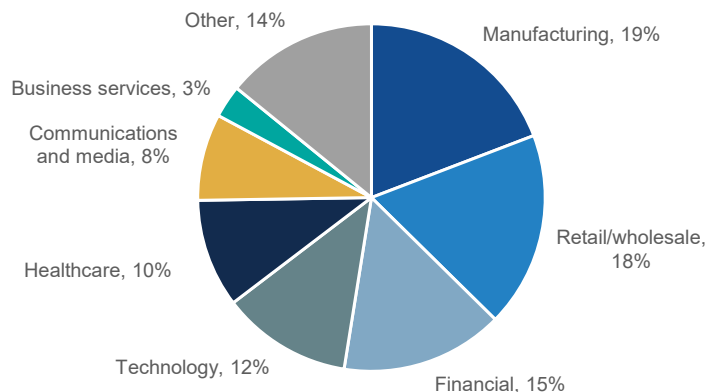


Figure 19. Vertical Sectors Represented

(Percent of respondents, N=1,000)



Appendix II: Criteria for Evaluating Organizations' Maturity

To evaluate how an organization's hybrid, multi-cloud management maturity is correlated to outcomes, Enterprise Strategy Group developed a maturity model that put forward four pillars of maturity against which organizations could be assessed via 11 distinct data points reported in the survey. Organizations with a mature approach earned more maturity points, and those with an immature approach earned fewer. Based on the answers to these questions, respondents' organizations could earn a maximum of 105 maturity points.

Leading organizations were defined as those organizations earning more than 80 maturity points, Converging organizations as those that earned between 70.25 and 80 points, Emerging organizations as those that earned between 60 and 70 points, and Nascent organizations as those that earned fewer than 60 points.

The questions asked to assess digital work technology maturity are shown in the following figures, along with the number of maturity points ascribed to each response.

Figure 20. Actions Taken to Converge Cloud Networking and Security Staff (Percent of respondents, N=1,000, multiple responses accepted)

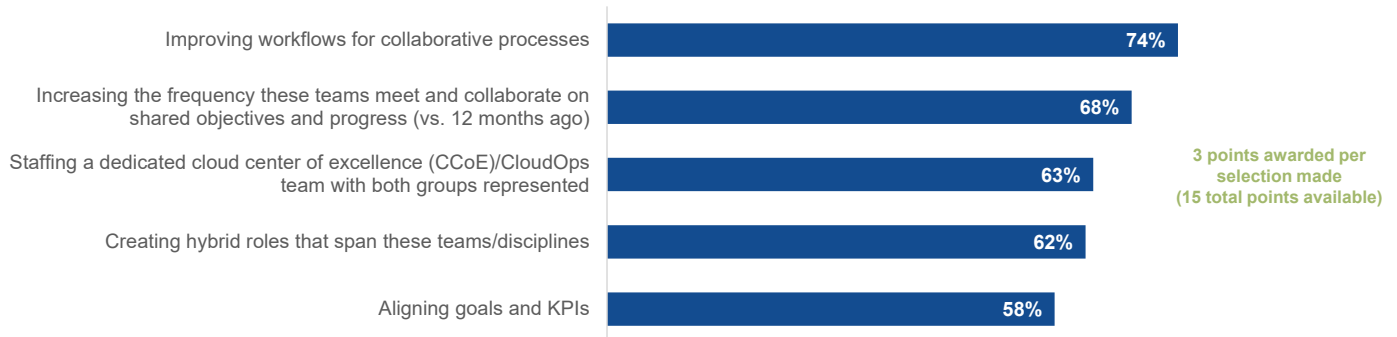


Figure 21. The State of Network and Security Teams' Collaboration (Percent of respondents, N=1,000)

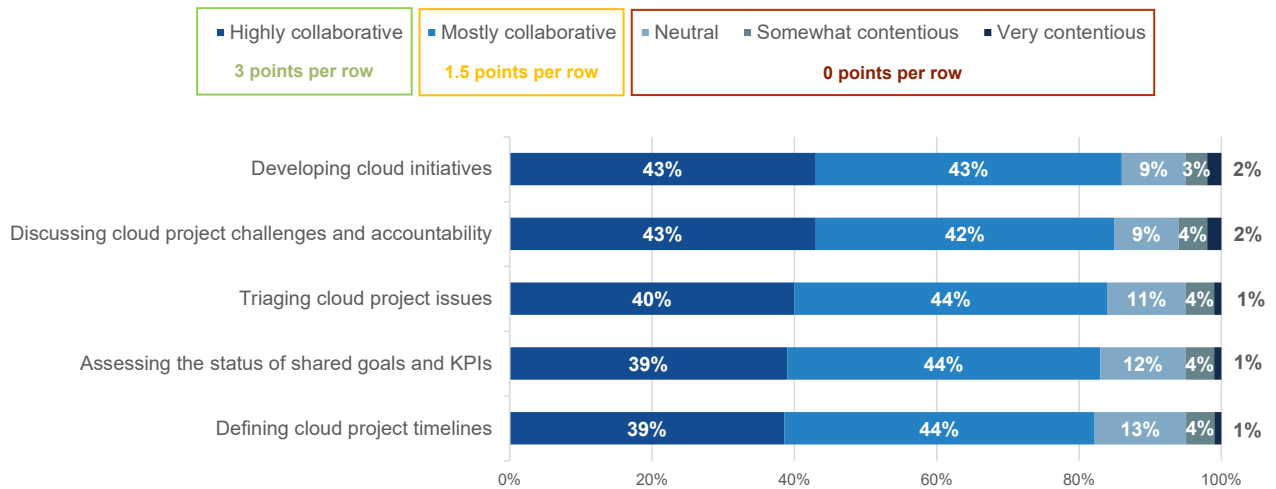


Figure 22. The State of Tool Convergence (Percent of respondents, N=1,000)

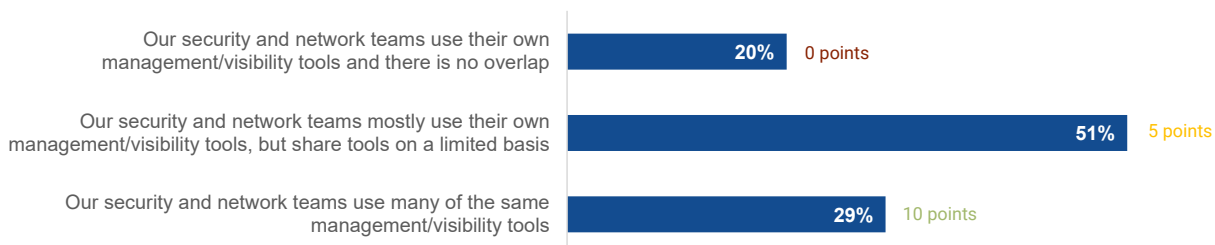


Figure 23. Organizations' Establishment of a Platform Engineering Team
(Percent of respondents, N=1,000)

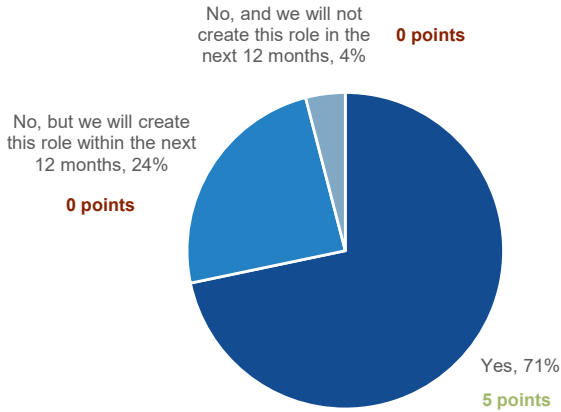


Figure 24. Maturity of the Platform Engineering Team
(Percent of respondents, N=1,000)

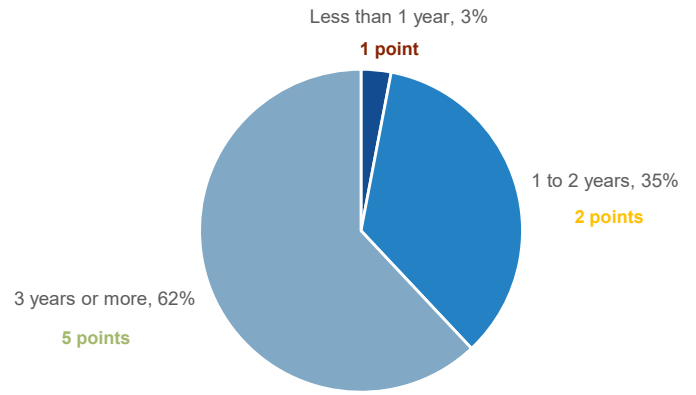


Figure 25. Cloud DDI Solution(s) in Use
(Percent of respondents, N=1,000)

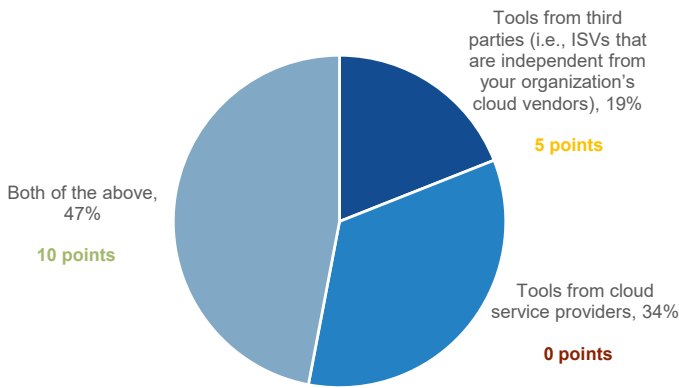


Figure 26. Cloud DDI Solution Most Relied Upon
(Percent of respondents, N=1,000)

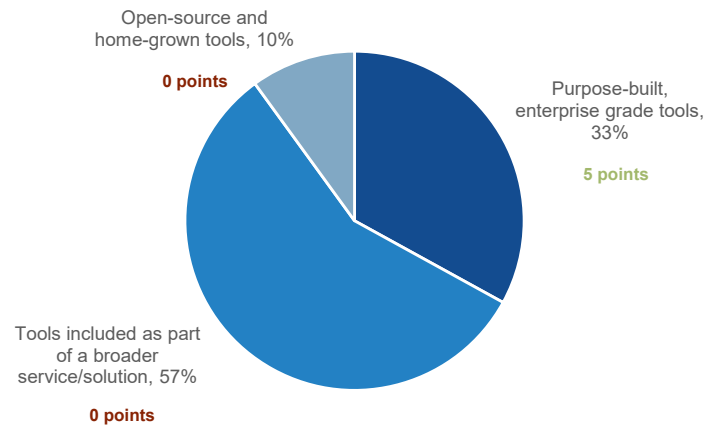


Figure 27. Cloud NetOps Automation (Percent of respondents, N=1,000)

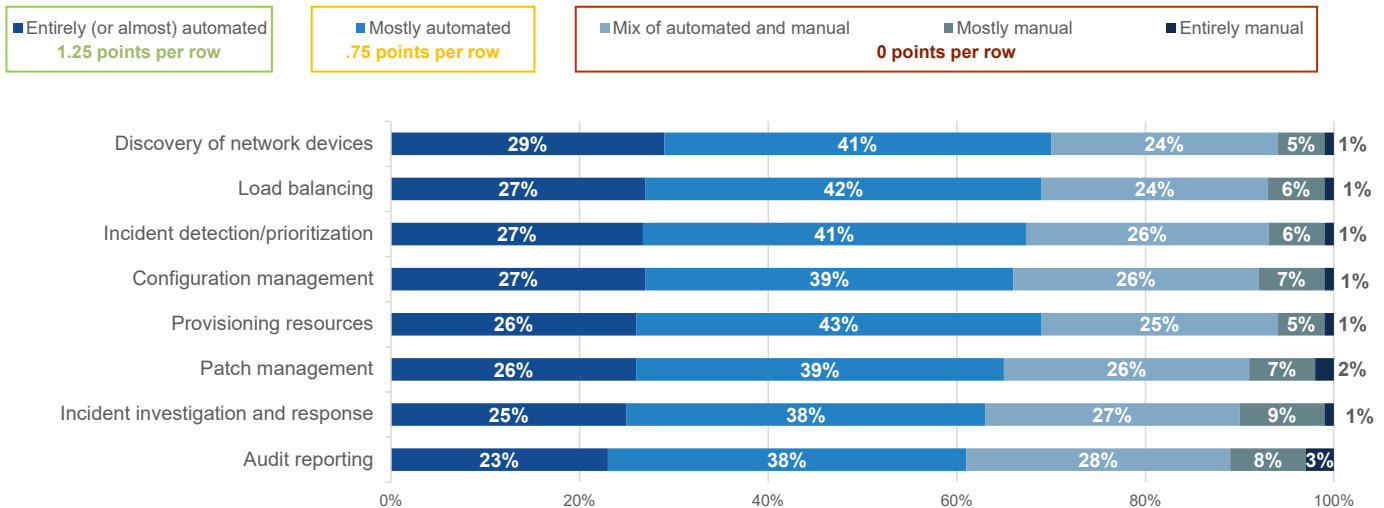


Figure 28. Cloud Security Solutions in Use (Percent of respondents, N=1,000)



Figure 29. Use of DNS for Security Use Cases (Percent of respondents, N=1,000)

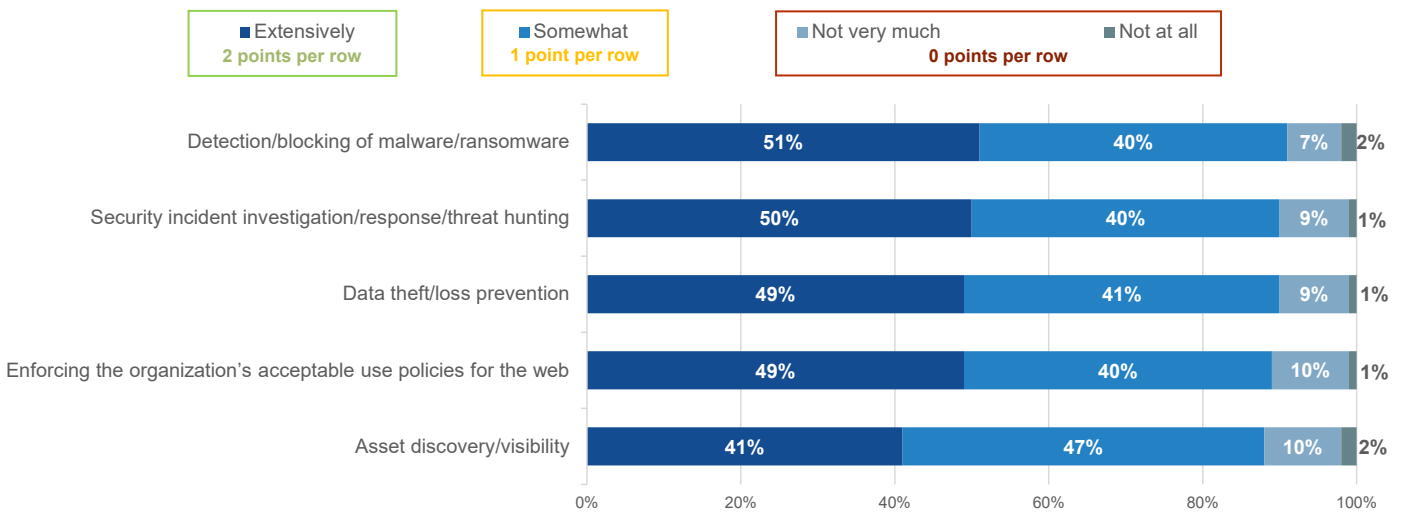
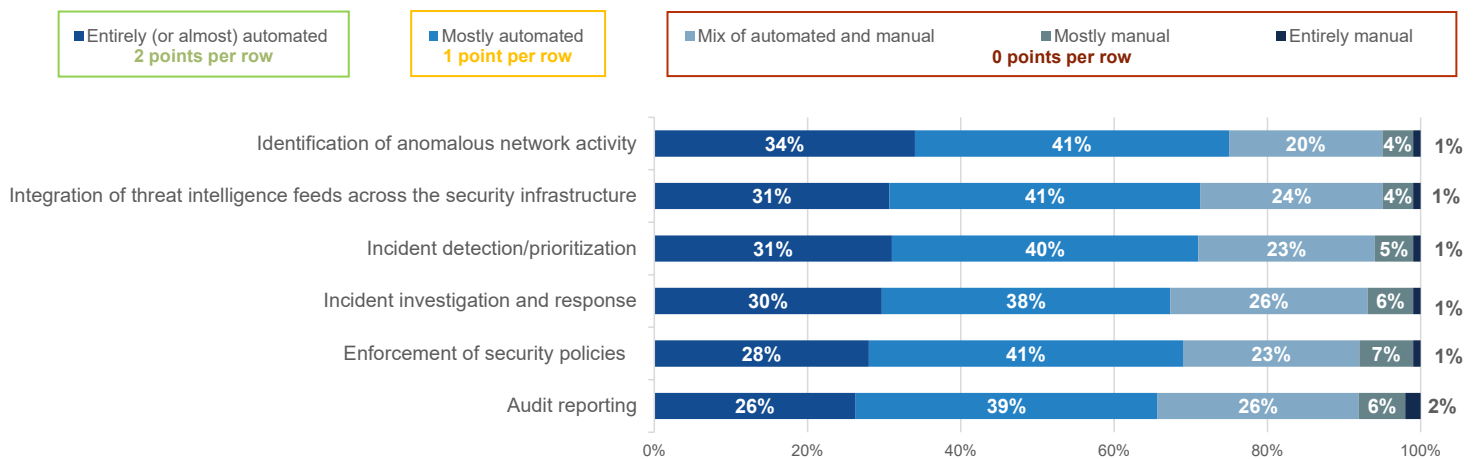


Figure 30. Cloud SecOps Automation (Percent of respondents, N=1,000)



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.